I claim:

1. A method of securely distributing game programs for execution in an electronic game system comprising the following steps:

(a) storing in a program storage medium a first game program that is encrypted under control of an encryption key;

(b) storing in a first semiconductor processor chip a decryption key corresponding to said encryption key;

(c) encrypting said decryption key in said first processor chip to produce an encrypted decryption key;

(d) transferring said encrypted decryption key from said first processor chip to a second processor chip;

(e) decrypting said encrypted decryption key in said second processor chip to reproduce said decryption key in said second processor chip;

(f) decrypting in said second processor chip said encrypted game program under control of said decryption key to produce executable digital instructions stored in said second processor chip; and

(g) executing said digital instructions in said second processor chip to generate game data that specifies to said game system at least one variable characteristic of a player controlled object, wherein said executable digital instructions are inaccessible from said second processor chip.

2. The method of claim 1, wherein said program storage medium and said first processor chip are housed in a cartridge that is manually removable from said game system.

3. The method of claim 1, wherein said encryption key and said decryption key are one symmetric key.

4. The method of claim 1, wherein said program storage medium is a semiconductor memory.

5. The method of claim 1, wherein said program storage medium is an optically readable disk.

6. The method of claim 1, wherein said first processor chip is removably connected to said game system during execution of at least some of said decrypted digital instructions.

7. The method of claim 1, wherein said first processor chip is disconnected from said game system during execution of at least some of said decrypted digital instructions.

8. The method of claim 1, wherein said second processor chip is firmly attached to said game system.

9. The method of claim 1, wherein said first processor chip is housed in a game cartridge that is removably connected to said game system during execution of said decrypted digital instructions.

10. The method of claim 1, further comprising the step of generating a session key in said second processor chip to control said encrypting of said decryption key in said first processor chip.

11. The method of claim 1, wherein said encrypted key is transferred from said first processor chip to said second processor chip under control of a session key randomly generated in said second processor chip and communicated in encrypted form to said first processor chip.

12. The method of claim 1, wherein said player controlled object is an animated character with articulated appendages that are programmed to move in response to manual operation of at least one control device in said portable game system.

13. The method of claim 1, wherein said game data specifies a location of an object in a simulated world.

14. The method of claim 1, wherein said game data specifies a location and an orientation of said player controlled object in a simulated world.

15. The method of claim 1, wherein said game data specifies a movement direction of a player controlled object in a simulated world.

16. The method of claim 1, wherein said game data specifies a point of view location in a simulated world.

17. The method of claim 1, wherein said game data specifies a location of a non-player object in a simulated world.

18. The method of claim 1, wherein said game data represents an image of at least a portion of a player controlled object.

19. The method of claim 1, wherein said game system comprises an LCD device.

20. The method of claim 1, wherein at least some of said executable digital instructions are stored in said second processor chip in non-volatile read/write memory.

21. A cryptographic cartridge for protecting an encrypted program, the cartridge comprising:

(a) a housing arranged for manual insertion into a game system;

(b) a program storage medium in said housing storing said encrypted program;

(c) a cryptographic processor chip in said housing;

(d) non-volatile data memory in said processor chip for storing at least a first decryption key that is inaccessible from said processor chip and which is used to decrypt said encrypted program;

(e) decryption means in said processor chip to decrypt an input encrypted session key under control of a second decryption key to produce a decrypted session key that is inaccessible from said processor chip; and

(f) encryption means in said processor chip to encrypt said first decryption key under control of said decrypted session key to produce an encrypted decryption key that is output from said housing.

22. The cartridge of claim 21, wherein said program storage medium is a semiconductor memory.

23. The cartridge of claim 21, wherein said program storage medium is an optically readable disk.

24. The cartridge of claim 21, wherein said cartridge is removably connected to said game system during decryption of said encrypted program in said game system.

25. The cartridge of claim 21, wherein said cartridge is disconnected from said game system during execution of said decrypted program.

26. The cartridge of claim 21, wherein said encrypted decryption key is transferred from said processor chip to a second processor chip in said game system, wherein the second processor chip randomly generates said session key and encrypts said session key.

27. A cryptographic cartridge for protecting an encrypted program, the cartridge comprising:

(a) a housing arranged for manual insertion into a game system;

(b) a program storage medium in said housing that stores said encrypted program;

(c) a decryption key stored in encrypted form in said program storage medium for decrypting said encrypted program;

(d) a crypto processor chip in said housing; and

(e) encryption means in said processor chip to encrypt said decryption key to produce an encrypted decryption key that is output from said housing.

28. The cartridge of claim 27, wherein said program storage medium is a semiconductor memory.

29. The cartridge of claim 27, wherein said program storage medium is an optically readable disk.

30. The cartridge of claim 27, wherein said cartridge is removably connected to said game system during decryption of said encrypted program in said game system.

31. The cartridge of claim 27, wherein said cartridge is disconnected from said game system during execution of said program in said game system.

32. The cartridge of claim 27, wherein said encrypted decryption key is transferred from said crypto processor chip to a second crypto processor chip in said game system.

33. A cryptographic system comprising a first processor chip and a second processor chip,

said first processor chip:

generating a session key;

encrypting said session key; and

transferring the encrypted session key to said second processor chip;

said second processor chip:

storing a game program decryption key;

decrypting said encrypted session key;

encrypting said game program decryption key under control of said decrypted session key; and

transferring said encrypted decryption key to said first processor chip;

said first processor chip:

decrypting said encrypted decryption key under control of said session key to produce said game program decryption key;

decrypting an encrypted game program under control of said game program decryption key to produce decrypted game program instructions; and

executing said decrypted game program instructions in said first processor chip.

34. The system of claim 33, wherein said encrypted game program is stored in a program storage medium that is housed with said second processor chip in a game cartridge.

35. A method of securely distributing a game program for execution in an electronic game system comprising the following steps:

(a) storing an encrypted game program in a program storage medium in a portable housing that also houses a first processor chip that contains a unique identifier;

(b) encrypting said unique identifier in said first processor chip to produce an encrypted identifier;

(c) transmitting said encrypted identifier from said first processor chip through a data communications network to a server that supplied said encrypted game software;

(d) decrypting said encrypted identifier in said server to produce a decrypted identifier;

(e) reencrypting in said server said decrypted identifier and a digital key corresponding to said encrypted game software to produce at least one encrypted data block;

(f) decrypting in said electronic game system said encrypted data block in a second processor chip that contains said unique identifier to produce a decrypted identifier and a decrypted key in said second processor chip;

(g) decrypting said encrypted game program in said second processor chip under control of said decrypted key to produce executable digital instructions if said decrypted identifier has a predetermined relationship with said unique identifier in said second processor chip.

36. The method of claim 35, wherein said portable housing is a game memory cartridge that is manually removable from said electronic game system.

37. The method of claim 35, wherein said program storage medium is a semiconductor memory.

38. The method of claim 35, wherein said program storage medium is an optically readable disk.

39. The method of claim 35, wherein said data communications network comprises a retailer computer that stores said encrypted data block into a data storage medium in said portable housing.

40. The method of claim 35, wherein said data communications network comprises a retailer computer that stores said encrypted game program into said program storage medium in said portable housing.

41. The method of claim 35, wherein said decrypted identifier and said digital key are reencrypted together in the same encrypted data block.

42. The method of claim 35, wherein said decrypted identifier and said digital key are reencrypted in separate encrypted data blocks.

43. The method of claim 35, wherein said first processor chip is removably connected to said game system during execution of at least some of said decrypted digital instructions.

44. The method of claim 35, wherein said first processor chip is disconnected from said game system during execution of at least some of said decrypted digital instructions.

45. The method of claim 35, wherein said second processor chip is firmly attached to said game system.

46. The method of claim 35, wherein said first processor chip is housed in a game cartridge that is removably connected to said game system during execution of said decrypted digital instructions.

47. The method of claim 35, further comprising the step of generating a session key in said server to control said encrypting of said unique identifier in said first processor chip.

48. The method of claim 35, wherein said encrypted identifier is transferred from said first processor chip to said server under control of a session key randomly generated in said server and communicated in encrypted form to said first processor chip.

49. The method of claim 35, wherein at least some of said executable digital instructions are executed in a processor core in said second processor chip.

50. The method of claim 35, further comprising the step of executing said digital instructions in said second processor chip to generate game data that specifies to said game system at least one variable characteristic of a player controlled object, wherein said executable digital instructions are inaccessible from said second processor chip.

51. The method of claim 50, wherein said player controlled object is an animated character with articulated appendages that are programmed to move in response to manual operation of at least one control device in said game system.

52. The method of claim 50, wherein said game data specifies a location of an object in a simulated world.

53. The method of claim 50, wherein said game data specifies a location and an orientation of said player controlled object in a simulated world.

54. The method of claim 50, wherein said game data specifies a movement direction of a player controlled object in a simulated world.

55. The method of claim 50, wherein said game data specifies a point of view location in a simulated world.

56. The method of claim 50, wherein said game data specifies a location of a non-player object in a simulated world.

57. The method of claim 50, wherein said game data represents an image of at least a portion of a player controlled object.

58. The method of claim 50, wherein said game system further comprises a discrete display device for displaying said player controlled object moving in response to manual operation of at least one control device attached to said game system.

59. A cryptographic cartridge for protecting an encrypted program, the cartridge comprising:

(a) a housing arranged for manual insertion into a game system;

(b) a program storage medium in said housing that stores said encrypted program;

(c) a decryption key stored in encrypted form in said housing for controlling decryption of said encrypted program;

(d) a crypto processor chip in said housing;

(e) a unique chip identifier in said crypto processor chip; and

(f) encryption means in said crypto processor chip to encrypt said unique chip identifier to produce an encrypted identifier that is output from said housing.

60. The cartridge of claim 59, wherein said program storage medium is a semiconductor memory.

61. The cartridge of claim 59, wherein said program storage medium is an optically readable disk.

62. The cartridge of claim 59, wherein said cartridge is removably connected to said game system during decryption of said encrypted program in said game system.

63. The cartridge of claim 59, wherein said cartridge is disconnected from said game system during execution of said program in said game system.

64. The cartridge of claim 59, wherein said encrypted decryption key is transferred from said cartridge to a second crypto processor chip in said game system.

65. A method of securely distributing game programs for execution in an electronic game system comprising the following steps:

(a) storing in a program storage medium a first game program that is encrypted under control of an encryption key;

(b) storing in a first semiconductor processor chip a decryption key corresponding to said encryption key;

(c) encrypting said decryption key in said first processor chip to produce an encrypted decryption key;

(d) transferring said encrypted decryption key from said first processor chip to a second processor chip;

(e) decrypting said encrypted decryption key in said second processor chip to reproduce said decryption key in said second processor chip;

(f) decrypting in said second processor chip said encrypted game program under control of said decryption key to produce executable digital instructions; and

(g) executing said digital instructions to generate game data that specifies to said game system at least one variable characteristic of a player controlled object.

66. The method of claim 65, wherein said program storage medium and said first processor chip are housed in a cartridge that is manually removable from said game system.

67. The method of claim 65, wherein said encryption key and said decryption key are one symmetric key.

68. The method of claim 65, wherein said program storage medium is a semiconductor memory.

69. The method of claim 65, wherein said program storage medium is an optically readable disk.